

UNITED STATES DISTRICT COURT

for the
Northern District of Oklahoma

FILED

AUG 15 2022

Mark C. McCartt, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of
Information Associated with the Kik Account
"ebromanee" that is Stored at a Premises Controlled by
MediaLab.AI Inc.

Case No. 22-mj-509-SH

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A."

This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).

Located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

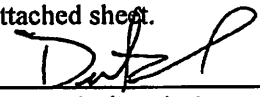
18 U.S.C. §§ 2252(a)(4)(B)

Possession of Child Pornography

The application is based on these facts:

See Affidavit of SA Dustin L. Carder, HSI, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Dustin Carder, Special Agent, HSI

Printed name and title

Sworn to before me and signed ^{by telephone} ~~in my presence~~.

Date: 8/15/22


Judge's signature

City and state: Tulsa, Oklahoma

Susan E. Huntsman, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
Information Associated with the Kik
Account “ebromanee” that is Stored at
a Premises Controlled by MediaLab.AI
Inc.**

Case No. _____

Affidavit in Support of an Application for a Search Warrant

I, Dustin L. Carder, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at a premises owned, maintained, controlled, or operated by MediaLab.AI Inc., an electronic communications service and/or remote computing service provider headquartered at 1237 7th Street, Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent (“SA”) with Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”) since December 2018 and am currently assigned to the Office of the Resident Agent in Charge in Tulsa, Oklahoma, and am currently assigned to investigate crimes involving child exploitation. While employed by HSI, I have investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center’s (FLETC) twelve-week Criminal Investigator Training Program (CITP) and the sixteen-week Homeland Security Investigations Special Agent Training (HSISAT) program, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received focused child exploitation training covering topics such as: interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex offenders, and mobile messaging platforms utilized by these types of offenders. Moreover, I am a

federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 1470, 2251, 2252, 2252(a), and 2422.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of certain material involving the sexual exploitation of a minor) have been committed by Kik user “ebromanee.” There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes, as further described in Attachment B.

Jurisdiction

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States

... that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

7. When the government obtains records pursuant to § 2703, or pursuant to a search warrant, the government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally, the government may obtain an order precluding MediaLab from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

Probable Cause

8. On July 29, 2022, I was contacted by Gabriel Thrasher, Senior U.S. Probation Officer for the Northern District of Oklahoma, in reference to assisting him review the contents of a phone seized from Mikaili COHN. On October 31, 2017, COHN was convicted in the Northern District of Oklahoma for violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of child pornography) under case number 16-CR-00139-GKF. COHN was sentenced to a term of 48 months in the custody of the Bureau of Prisons followed by a term of 20 years of supervised release. COHN commenced supervision on May 6, 2020.

9. COHN’s Special Conditions of Supervision (numbers 4-6 and 8) state that:

- a. The defendant shall not possess or view photographs, images, books, magazines, writings, drawings, videos, or video games depicting or describing sexually explicit conduct or child pornography, as defined in 18 U.S.C. § 2256(2) or § 2256(8), or patronize places where such materials or images are available.
- b. The defendant shall submit his/her person, property, residence, office, vehicle, papers, computers (as defined in 18 U.S.C. § 1030(e)(1)), electronic communication devices, data storage devices, or media, to a search, conducted by the probation officer at a reasonable time and in a reasonable manner, based on a reasonable suspicion of contraband or evidence of a violation of a condition of release (except as set forth in the Computer and Internet Restriction Condition (Paragraph 8(b)), if imposed). Failure to submit to a search may be grounds for revocation. The defendant shall warn any other occupants that the premises may be subject to searches pursuant to this condition.
- c. The defendant shall only use electronic communications devices or data storage devices approved in advance by the probation officer and accessible to a complete forensic search by the Probation Office.
- d. The defendant shall abide by the following computer restrictions and monitoring conditions:
 - i. The defendant shall disclose all e-mail accounts, internet connections and internet connection devices, including screen

names, user identifications, and passwords, to the probation officer; and shall immediately advise the probation officer of any changes in his/her email accounts, connections, devices, or passwords.

- ii. The defendant shall allow the probation officer to install computer monitoring software on any computer, as defined by 18 U.S.C. § 1030(e)(1), that the defendant owns, utilizes or has the ability to access. To ensure compliance with the computer monitoring condition, the defendant shall allow the probation officer to conduct periodic, unannounced searches of any computer subject to computer monitoring. These searches shall be conducted for the purposes of determining whether the computer contains any prohibited data prior to installation of the monitoring software; to determine whether the monitoring software is functioning effectively after its installation; and to determine whether there have been attempts to circumvent the monitoring software after its installation. Additionally, the defendant shall warn other people who use these computers that the computers may be subject to searches pursuant to this condition.
- iii. The defendant shall not access any on-line service using an alias, or access any on-line service using the internet account, name, or designation of another person or entity; and shall report immediately to the probation officer access to any internet site containing prohibited material.
- iv. The defendant is prohibited from using any form of encryption, cryptography, stenography, compression, password protected files or other methods that limit access to, or change the appearance of, data and/or images.
- v. The defendant is prohibited from altering or destroying records of computer use, including the use of software or functions designed to alter, clean or “wipe” computer media, block monitoring software, or restore a computer to a previous state.

10. On July 12, 2022, U.S. Probation Officers arrested COHN at 11206 East Brady Street, Apartment 224, Tulsa, Oklahoma, within the Northern District of

Oklahoma, on a charge of Failure to Register as a Sex Offender in relation to supervision violations. Supervisory Probation Officer Kory McClintock observed an Apple iPhone (S/N#C8PZP3Q7N72N) on a dresser in COHN's room at the location. Officer McClintock asked COHN's girlfriend if the phone was hers; she said it was not. Officer McClintock then seized the phone.

11. Probation Officer Thrasher had the phone forensically examined at the U.S. Probation Office and began reviewing the contents. In the data, Officer Thrasher located a conversation that occurred on Kik between users "ebromanee" and "boredgeezus" during the timeframe of July 9, 2022, through July 11, 2022. Username "ebromanee" was found to be the account located on the iPhone that was seized from COHN's bedroom.

12. The conversation is listed below:

- a. **Boredgeezus:** If anyone wants a mega¹ link w over 250gb on it PM me
- b. **Ebromanee:** Send it
- c. **Boredgeezus:** 8ts not free
- d. **Boredgeezus:** ?
- e. **Ebromanee:** How much

¹ MEGA is a cloud storage and file hosting service offered by MEGA Limited, a company based in Auckland, New Zealand. The service is offered through web-based apps. MEGA mobile apps are also available for Android and iOS. MEGA offers its users a limited amount of free cloud storage and end-to-end encryption. Although it has legitimate uses, MEGA is widely abused and is often used for the distribution, receipt, and storage of child pornography.

- f. **Boredgeezus:** \$25
- g. **Boredgeezus:** I'll do 20
- h. **Boredgeezus:** ?
- i. **Ebromanee:** Okay I'd like to preview the link before I pay. Like 5 mins then kill the link so I know what I'm buying. I buy Cp² all the time
- j. **Boredgeezus:** Lmao that's funny
- k. **Boredgeezus:** I know what importing to the cloud is you fucking idiot
- l. **Ebromanee:** I must be an idiot bc idk what your talking about, but I've bought before. Sometimes I'm scammed sometimes I'm not is all

13. As evidenced by the above chat, user ebromanee has purchased child pornography before and was seeking it out on the Kik application. COHN's original conviction stems from a 2016 HSI investigation where COHN distributed child pornography to an undercover HSI agent via the Kik application. His username at that time was "gocheezy." This same username was found on the seized iPhone for the social media application Snapchat as well as multiple websites.

14. On July 3, 2022, COHN entered a search query in the iPhone's Safari web browser for "duetsch incest lolita." Based on my training and experience, I know that "lolita" is a term also often associated with child pornography.

² Based on my training and experience in working child exploitation investigations, I know that "cp" refers to child pornography and that Kik is widely used in the distribution of child pornography.

15. On August 1, 2022, I preserved the contents of ebromanee's Kik account under preservation request number "KIK-6444." On August 4, 2022, I met with Officer Thrasher and took a copy of the phone dump for additional review. In reviewing the data, I located the same information described above as related by Officer Thrasher. I did not locate any images or videos of child pornography in the extracted data.

16. In addition to confirming Officer Thrasher's findings on the iPhone, I located email addresses of mikailicohn@pm.me, and nightbanter@protonmail.com that were used as Apple IDs³ on the device. Based on my review of the phone data, it appears that the nightbanter@protonmail.com email account is related to a podcast that COHN was doing or planning to do.

17. On or about August 8, 2022, I electronically served MediaLab with an administrative Department of Homeland Security summons for subscriber information related to the account. MediaLab responded the same day and provided the requested information. The ebromanee account was registered on May 26, 2022, with the email address of 100tropwen@gmail.com.

18. As evidenced herein, the iPhone was utilized by COHN, it was an unauthorized device according to the terms of his supervision, he utilized Kik

³ Apple ID is an authentication method used by Apple for iPhone, iPad, Mac, and other Apple devices. Apple IDs contain user personal information and settings. When an Apple ID is used to log in to an Apple device, the device will automatically use the settings associated with the Apple ID.

previously in the distribution of child pornography, and according to one conversation located on his device, he was currently using Kik to procure/attempt to procure child pornography.

19. For these reasons, I believe that a search of COHN's Kik account is likely to reveal child pornography and other individuals with whom he has communicated in the receipt, distribution, and possession of child pornography. I know from previous child exploitation investigations involving the Kik application, that media content, as well as with whom that content is shared, is often stored by Kik (MediaLab) and able to be produced upon the service of a search warrant.

Background Concerning Kik

20. Kik advertises itself as "the first smartphone messenger with a built-in browser." Kik Messenger allows its users to "talk to your friends and browse and share any web site with your friends on Kik." Kik believes it is at the forefront of the "new era of the mobile web." Kik was founded in 2009 by a group of University of Waterloo students who started a company designed to "shift the center of computing from the PC to the phone." According to the website, Kik Messenger, a free service easily downloaded from the Internet, has become the simplest, fastest, most life-like chat experience you can get on a smartphone. Unlike other messengers, Kik usernames - not phone numbers - are the basis for Kik user accounts, so Kik users are in complete control with whom they communicate. In addition, Kik features include

more than instant messaging. Kik users can exchange images, videos, sketches, stickers, and even more with mobile web pages.

21. The Kik app is available for download via the App Store for most iOS devices such as iPhones and iPads. Additionally, the Kik app is available on the MediaLab PlayStore for Android devices. Kik can be used on multiple mobile devices, to include cellular phones and tablets.

22. In general, providers like Kik ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address.

23. Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

24. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems or complaints from other users. Providers typically retain records about such communications, including records of e-mails and other contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

25. As explained below, information stored at MediaLab, parent company of Kik, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to an account that is retained by a provider like Kik can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up- and other communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a Kik account at a relevant time. Further, such stored electronic data can show how and when the account was accessed or used. Such "timeline" information allows investigators to understand the chronological context of the usage of an account, account access, and events relating to the crime under investigation. This "timeline" information may tend to either inculcate or

exculpate the user of a Kik account. Additionally, stored electronic data may provide relevant insight into the state of mind of the user of a phone number as it relates to the offense under investigation. For example, information relating to a particular Kik account may indicate the user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

26. Kik offers users the ability to create an identity within the app referred to as a "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to obtain a different username. The username for a particular Kik account holder is generally displayed in their Kik profile.

27. In October 2019, Kik was purchased by MediaLab.AI Inc., a company operating in the United States.

28. In my training and experience, evidence of who was using a Kik account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

29. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of

criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Kik account may provide direct evidence of the offenses under investigation.

30. In addition, the user's account activity, logs, stored electronic communications, and other data retained by MediaLab can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time and can aid in locating the targets of an investigation. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

31. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of

guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

Information to be Searched and Things to be Seized

32. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on MediaLab. Because the warrant will be served on MediaLab, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

33. Affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require MediaLab to disclose to the government digital copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

34. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime under investigation, including but not limited to undertaking a cursory inspection of all information

within the account described in Attachment A. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, Affiant knows that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but do not contain any searched keywords.

Conclusion

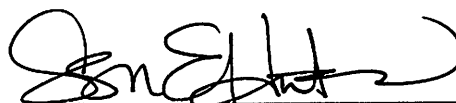
35. Based on the information above, there is probable cause to believe that there is evidence, instrumentalities, contraband, and/or fruits of these crimes, as described in Attachment B, of violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of certain material involving the sexual exploitation of a minor) associated with the Kik account described in Attachment A.

Respectfully submitted,



Dustin L. Carder
Special Agent
Homeland Security Investigations

Subscribed and sworn to by phone on August 15, 2022.



SUSAN E. HUNTSMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Kik account “**ebromanee**” (“the Account”) that is stored at premises owned, maintained, controlled, or operated by MediaLab.AI Inc., a company headquartered at 1237 7th Street, Santa Monica, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by MediaLab.AI Inc. (“MediaLab”)

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to MediaLab, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on August 1, 2022, under KIK-6444, MediaLab is required to disclose to the government for each account or identifier listed in Attachment A the following information for the timeframe of May 26, 2022, through July 12, 2022, unless otherwise indicated:

- a. The contents of all messages associated with the account, including stored or preserved copies of messages sent to and from the account, the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message;
- b. Any and all images, videos or other media sent and received by Kik account username “ebromanee”;
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-

in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including credit or bank account number);

- d. The types of service utilized;
- e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of certain material involving the sexual exploitation of a minor), those violations involving Kik user “ebromanee” and occurring between May 26, 2022 and July 12, 2022, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The receipt and/or distribution of child pornography;
- b. The possession of child pornography;
- c. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use,

and events relating to the crime under investigation and to the email account owner;

- d. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;**
- e. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).**
- f. The identity of the person(s) who communicated with the Account about matters relating to the possession, distribution, and receipt of child pornography, including records that help reveal their whereabouts.**

Certificate of Authenticity of Domestic Records Pursuant to Federal Rules of Evidence 902(11) and 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by MediaLab.AI Inc. (“MediaLab”), and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of MediaLab. The attached records consist of _____ gigabytes of data. I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of MediaLab, and they were made by MediaLab as a regular practice; and

b. Such records were generated by MediaLab’s electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of MediaLab in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by MediaLab, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature